

EXHIBIT 5

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
<p>A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:</p> <p>receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;</p>	<p>Cisco Advanced Malware Protection (AMP) includes <i>a non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information</i> (e.g., a smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof, including associated information including but not limited to information describing the actual vulnerabilities themselves, information describing endpoints that contain the particular operating system/application/version thereof, information describing policy/detection/remediation techniques for addressing the actual vulnerabilities relevant to the particular operating system/application/version thereof including signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) <i>from at least one first data storage</i> (e.g., memory on the at least one device storing a repository of the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof, etc.) <i>that is generated utilizing second vulnerability information</i> (e.g., a larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof, including associated information including but not limited to information describing the possible vulnerabilities themselves, information describing the different operating systems/applications/versions thereof, information describing policy/detection/remediation techniques for addressing the potential vulnerabilities relevant to the different operating systems/applications/versions thereof including signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) <i>from at least one second data storage</i> (e.g., a Common Vulnerabilities and Exposures (CVE) database, etc.) <i>that is used to identify a plurality of potential vulnerabilities</i> (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.);</p> <p>Note: See, for example, the evidence below (emphasis added, if any):</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<ul style="list-style-type: none"> “AMP Cloud provides access to the <u>global intelligence database that is constantly updated</u> and augmented with new detections and provides a great breadth of knowledge to the AMP Connector through one-to-one hash lookups, a generic signature engine, and the machine learning engine.” <div data-bbox="669 548 1703 1008"> <p>The diagram illustrates the progression of detection stages for AMP Cloud. A horizontal arrow at the top indicates the 'Time to detection', ranging from 'Shorter' on the left to 'Longer' on the right. Below this arrow are three main categories of detection, each represented by a light blue box containing specific components:</p> <ul style="list-style-type: none"> In memory (green boxes): <ul style="list-style-type: none"> Exploit prevention System process protection On disk (blue boxes): <ul style="list-style-type: none"> AMP cloud Malicious activity protection TETRA Custom detections Post - infection (orange boxes): <ul style="list-style-type: none"> Cognitive threat analytics Device flow correlation Cloud IOCs Endpoint IOCs </div> <p>https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.pdf</p> <p>“Compromises</p> <p>By definition, <u>compromises represent potentially malicious activity that has been detected by AMP</u> that has not been quarantined but that may require action on your part. Compromises are displayed through a heat map showing groups with compromised computers and a time graph</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability						
	<p>showing the number of compromises for each day or hour over the past 14 days. Click the Inbox link to view the compromises on the Inbox Tab and take steps to resolve them.” Cisco AMP for Endpoints User Guide, Chapter 1, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“Common Vulnerabilities and Exposures</p> <p>The Common Vulnerabilities and Exposures (CVE) database records <u>known vulnerabilities in various applications</u>. All vulnerabilities are noted by their unique CVE ID. The CVE ID shown in the Console can be clicked to get more details on the vulnerability.” Cisco AMP for Endpoints User Guide, Chapter 20, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p><u>“Designed for Cisco Firepower® network threat appliances</u>, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.” https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)</p> <p>“Features and Benefits of Cisco AMP for Endpoints”</p> <table border="1" data-bbox="661 1247 1896 1404"> <thead> <tr> <th data-bbox="661 1247 905 1287">Feature</th><th data-bbox="905 1247 1896 1287">Benefits</th></tr> </thead> <tbody> <tr> <td data-bbox="661 1287 905 1328">...</td><td data-bbox="905 1287 1896 1328">...</td></tr> <tr> <td data-bbox="661 1328 905 1404"><u>Dashboards</u></td><td data-bbox="905 1328 1896 1404">Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation</td></tr> </tbody> </table>	Feature	Benefits	<u>Dashboards</u>	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation
Feature	Benefits						
...	...						
<u>Dashboards</u>	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation						

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability	
		information, <u>as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities</u> - to provide a comprehensive contextual view so that you can make informed security decisions.

	Exploit Prevention	<u>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.</u> The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a payload, and zero-day attacks on software vulnerabilities yet to be patched.

	Vulnerabilities	Identify vulnerable software and close attack pathways. This feature <u>shows a list of hosts that contain vulnerable software, a list of the vulnerable software on each host, and the hosts most likely to be compromised.</u> Powered by our threat intelligence and security analytics, AMP identifies vulnerable software being targeted by malware, shows you the potential exploit, and provides you with a prioritized list of hosts to patch.
	https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)	
said first vulnerability information generated utilizing the second vulnerability information, by:	Cisco Advanced Malware Protection (AMP) includes <i>said first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>generated utilizing the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability		
<p>identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and</p>	<p>systems/applications/versions thereof), <i>by: identifying at least one configuration</i> (e.g., a Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>associated with a plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.) <i>including a first device, a second device, and a third device</i>, (e.g., a first, second, and third of the 50+ nodes licensed to use the software, etc.) <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Vulnerabilities</p> <p>Vulnerabilities are displayed through a heat map that <u>shows groups that include computers with known vulnerable applications installed.</u>”</p> <p>Cisco AMP for Endpoints User Guide, Chapter 1, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf Last Updated: December 14, 2020</p> <p>“Deployment Options for Protection Everywhere</p> <p>Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:”</p> <table border="1" data-bbox="663 1287 1906 1325"> <tr> <th data-bbox="663 1287 930 1325">Product Name</th><th data-bbox="930 1287 1906 1325">Details</th></tr> </table>	Product Name	Details
Product Name	Details		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability	
	Cisco AMP for Endpoints	Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP's lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.
	https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)	
	"Software requirements"	
	Cisco AMP for Endpoints	<ul style="list-style-type: none"> ● Microsoft <u>Windows XP</u> with Service Pack 3 or later ● Microsoft <u>Windows Vista</u> with Service Pack 2 or later ● Microsoft <u>Windows 7</u> ● Microsoft <u>Windows 8 and 8.1</u> ● Microsoft <u>Windows 10</u> ● Microsoft <u>Windows Server 2003</u> ● Microsoft <u>Windows Server 2008</u> ● Microsoft <u>Windows Server 2012</u> ● <u>Mac OS X</u> 10.7 and later ● <u>Linux Red Hat</u> Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3 ● <u>Linux CentOS</u> 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3
	Cisco AMP for Endpoints on <u>Android</u> mobile devices	<u>Android version 2.1</u> and later
	Cisco AMP for Endpoints on <u>Apple iOS</u>	MDM supervised <u>iOS version 11</u>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p>https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</p> <p>“Cisco’s AMP for endpoints subscription offerings begin with <u>a minimum of 50 nodes, and thus inherently the network would include a plurality of devices</u> (e.g., nodes, etc.), that include at least a first, second, and third device.”</p> <p>http://winncom.com.ua/wp-content/uploads/2018/06/Cisco-Advanced-Malware-Protection-for-Endpoints.pdf</p>
<p>determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;</p>	<p>Cisco Advanced Malware Protection (AMP) includes <i>determining that the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.) <i>is actually vulnerable to at least one actual vulnerability</i> (e.g., one of a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>based on the identified at least one configuration</i> (e.g., a Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.), <i>utilizing the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is used to identify the plurality of potential vulnerabilities</i> (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: Each node has “AMP for Endpoint” Connector software installed thereon that identifies the operating system/applications/versions thereof on such node and, based thereon, uses the second vulnerability information (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) to identify the plurality of potential vulnerabilities.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p>“Whenever an executable file is moved, copied, or executed the AMP for Endpoints Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database that information is displayed on the Vulnerable Software page.</p> <p>Currently the following applications and versions on Windows operating systems are reported on the vulnerabilities page:</p> <p>...</p> <p>By default, all known vulnerable programs are shown.</p> <p>...</p> <p>Additional information is available at the bottom of the expanded program list item. The following topics provide additional information through the associated links:</p> <ul style="list-style-type: none"> • Observed in Groups • Last Observed (computer) • Events • File Trajectory" <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 20, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p>
identify an occurrence in connection with at least one of the plurality of devices;	Cisco Advanced Malware Protection (AMP) is configured to <i>identify an occurrence</i> (e.g., a discrete event that triggers at least one of the signature/policy updates for the anti-virus, intrusion detection, and/or firewall software, etc.) <i>in connection with at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.);

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Correlate discrete events into coordinated attacks: Cisco AMP for Networks illustrates the risk associated with an ongoing attack. It provides automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources.” https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)</p>
<p>determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and</p>	<p>Cisco Advanced Malware Protection (AMP) is configured to <i>determine that the at least one actual vulnerability</i> (e.g., one of the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.) <i>is susceptible to being taken advantage of by the occurrence</i> (e.g., the discrete event that triggers at least one of the signature/policy updates for the anti-virus, intrusion detection, and/or firewall software, etc.) <i>identified in connection with the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>utilizing the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof); <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: The TETRA/ClamAV anti-virus software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device’s operating system) trigger a response.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p>“TETRA</p> <p>TETRA is a full antivirus replacement and should never be enabled if another antivirus engine is installed. TETRA can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment.</p> <p>To enable TETRA and adjust settings go to Advanced Settings > TETRA in your policy.” Cisco AMP for Endpoints User Guide, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“Detection Engines</p> <p>Windows, Mac, and Linux Connectors have the option of enabling offline detection engines (TETRA for Windows and ClamAV for Mac and Linux) to protect the endpoint from malware without connecting to the Cisco Cloud to query each file.” Cisco AMP for Endpoints User Guide, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>Note: The anti-intrusion software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device’s operating system) trigger a response.</p> <p>“Detect and Block Exploit Attempts</p> <p>Cisco AMP for Networks builds on the Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS). <u>When the system is deployed in line, it detects and blocks client-side exploit</u></p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p><u>attempts that can lead to malicious file downloads</u>, commonly referred to as drive-by attacks. The NGIPS system can also protect against other vulnerability exploit attempts aimed at web browsers, Adobe Acrobat, Java, Flash, and other commonly targeted client applications. Acting as early as possible in the attack chain, the system attempts to limit collateral damage and avoid costly cleanup efforts.”</p> <p>https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)</p> <p>“Exploit Prevention (Connector version 6.0.5 and later)</p> <p>The AMP for Endpoints Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a Custom Detections - Simple list.</p> <p>To enable the exploit prevention engine, go to Modes and Engines in your policy and select Audit or Block mode. Audit mode is only available on AMP for Endpoints Windows Connector 7.3.1 and later. Earlier versions of the Connector will treat Audit mode the same as Block mode.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 7, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“AMP for Endpoints Premier subscriptions include Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco AMP Efficacy Research Team to help identify threats found within the customer environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p>preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation.</p> <p>...</p> <p>Remediation includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 28, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>"AMP for Endpoints Exploit Prevention ...- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy." Chapter 1, https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf) Last Updated: April 2020</p> <p>Note: The firewall software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device’s operating system) trigger a response.</p> <p>“Firewall Connectivity</p> <p>To allow the AMP for Endpoints Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are three sets of servers depending on where you are located: one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world.</p> <p>IMPORTANT! If your firewall requires IP address exceptions, see this Cisco TechNote.”</p>

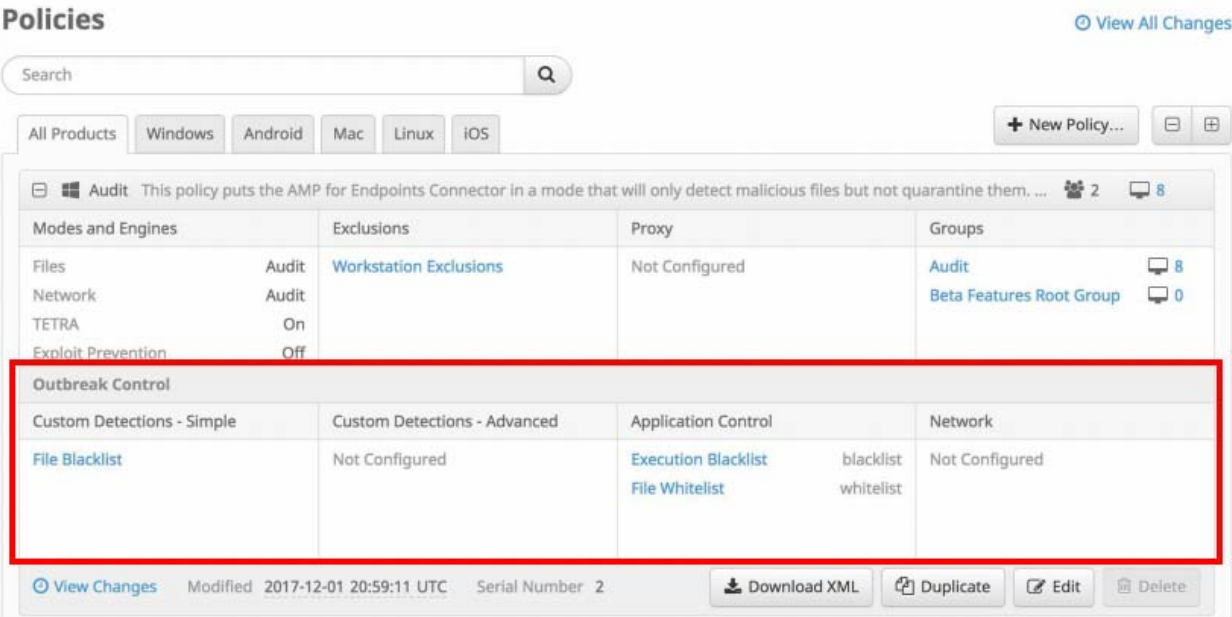
PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“AMP for Endpoints Windows Connector 7.0.5</p> <p>New</p> <ul style="list-style-type: none"> • Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications <ul style="list-style-type: none"> • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)” <p>Cisco <i>AMP for Endpoints Release Notes</i>, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)</p>
<p>cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation</p>	<p>Cisco Advanced Malware Protection (AMP) is configured to <i>cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types</i> (e.g., firewall software-, intrusion detection software-, anti-virus software-related actions, etc.), <i>including a firewall-based occurrence mitigation type</i> (e.g., firewall software-related actions including quarantining and/or blocking, etc.) <i>and a other occurrence mitigation type</i> (e.g., intrusion detection software-, anti-virus software-, or any other non-firewall software-related actions, etc.), <i>across the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.) <i>for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types</i> (e.g., firewall software-, intrusion detection software-, anti-virus software-related actions, etc.) <i>across the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.);</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
actions of the diverse occurrence mitigation types across the plurality of devices;	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Policy Summary</p> <p>Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.</p>  <p>View Changes will take you to a filtered view of the Audit Log showing all the changes for that specific policy. You can also use View All Changes at the top of the page to show changes to all policies.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<p>Click Edit to modify an existing policy or click Duplicate if you want to create a new policy with the same settings.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 4, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“Outbreak Control</p> <p>The Outbreak Control menu contains items related to controlling outbreaks in your network.</p> <ul style="list-style-type: none"> • Custom Detections <ul style="list-style-type: none"> ○ Simple to convict files that are not yet classified. ○ Advanced to create signatures that will detect parts of the Portable Executable (PE) file. ○ Android to warn of new threats or unwanted apps. • Application Control <ul style="list-style-type: none"> ○ Blocked Lists to stop executables from running. ○ Allowed Lists to create lists of applications that will not be wrongly detected. • Network <ul style="list-style-type: none"> ○ IP Blocked & Allowed Lists allow you to explicitly detect or allow connections to specified IP addresses. • Endpoint IOC <ul style="list-style-type: none"> ○ Initiate Scan to schedule and start IOC scans on your AMP for Endpoints Connectors (Administrator only). ○ Installed Endpoint IOCs to upload new endpoint IOCs and view installed endpoint IOCs (Administrator only). ○ Scan Summary to view the results of endpoint IOC scans. • Automated Actions

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	<ul style="list-style-type: none"> ○ Automated Actions lets you set actions that automatically trigger when a specified event occurs on a computer.” <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 1, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf Last Updated: December 14, 2020</p>
<p>wherein the at least one configuration involves at least one operating system.</p>	<p>Cisco Advanced Malware Protection (AMP) is configured <i>wherein the at least one configuration</i> (e.g., a Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>involves at least one operating system</i> (e.g., a Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Vulnerabilities</p> <p>Vulnerabilities are displayed through a heat map that <u>shows groups that include computers with known vulnerable applications installed.</u>”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 1, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf Last Updated: December 14, 2020</p> <p>“Deployment Options for Protection Everywhere</p> <p>Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, <u>the AMP solution can be deployed at different control points</u></p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability								
	<p><u>throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:</u></p> <table border="1"> <tr> <th>Product Name</th><th>Details</th></tr> <tr> <td>Cisco AMP for Endpoints</td><td><u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP's lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.</u></td></tr> </table> <p>https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)</p> <p>“Software requirements”</p> <table border="1"> <tr> <td>Cisco AMP for Endpoints</td><td> <ul style="list-style-type: none"> ● Microsoft <u>Windows XP</u> with Service Pack 3 or later ● Microsoft <u>Windows Vista</u> with Service Pack 2 or later ● Microsoft <u>Windows 7</u> ● Microsoft <u>Windows 8 and 8.1</u> ● Microsoft <u>Windows 10</u> ● Microsoft <u>Windows Server 2003</u> ● Microsoft <u>Windows Server 2008</u> ● Microsoft <u>Windows Server 2012</u> ● <u>Mac OS X</u> 10.7 and later ● <u>Linux Red Hat Enterprise</u> 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3 ● <u>Linux CentOS</u> 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3 </td></tr> <tr> <td>Cisco AMP for Endpoints on <u>Android</u> mobile devices</td><td><u>Android version 2.1</u> and later</td></tr> </table>	Product Name	Details	Cisco AMP for Endpoints	<u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP's lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.</u>	Cisco AMP for Endpoints	<ul style="list-style-type: none"> ● Microsoft <u>Windows XP</u> with Service Pack 3 or later ● Microsoft <u>Windows Vista</u> with Service Pack 2 or later ● Microsoft <u>Windows 7</u> ● Microsoft <u>Windows 8 and 8.1</u> ● Microsoft <u>Windows 10</u> ● Microsoft <u>Windows Server 2003</u> ● Microsoft <u>Windows Server 2008</u> ● Microsoft <u>Windows Server 2012</u> ● <u>Mac OS X</u> 10.7 and later ● <u>Linux Red Hat Enterprise</u> 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3 ● <u>Linux CentOS</u> 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3 	Cisco AMP for Endpoints on <u>Android</u> mobile devices	<u>Android version 2.1</u> and later
Product Name	Details								
Cisco AMP for Endpoints	<u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP's lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.</u>								
Cisco AMP for Endpoints	<ul style="list-style-type: none"> ● Microsoft <u>Windows XP</u> with Service Pack 3 or later ● Microsoft <u>Windows Vista</u> with Service Pack 2 or later ● Microsoft <u>Windows 7</u> ● Microsoft <u>Windows 8 and 8.1</u> ● Microsoft <u>Windows 10</u> ● Microsoft <u>Windows Server 2003</u> ● Microsoft <u>Windows Server 2008</u> ● Microsoft <u>Windows Server 2012</u> ● <u>Mac OS X</u> 10.7 and later ● <u>Linux Red Hat Enterprise</u> 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3 ● <u>Linux CentOS</u> 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3 								
Cisco AMP for Endpoints on <u>Android</u> mobile devices	<u>Android version 2.1</u> and later								

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability	
	Cisco AMP for Endpoints on <u>Apple iOS</u>	MDM supervised <u>iOS version 11</u> https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>The non-transitory computer-readable media of Claim 1, wherein the at least one actual vulnerability is one of the actual vulnerabilities that are of the at least operating system that is installed on the plurality of devices, the occurrence is at least one of a plurality of occurrences, and the instructions include:</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and includes <i>the non-transitory computer-readable media of Claim 1, wherein the at least one actual vulnerability</i> (e.g., one of a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>is one of the actual vulnerabilities that are of the at least operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>that is installed on the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.), <i>the occurrence</i> (e.g., the discrete event that triggers at least one of the signature/policy updates for the anti-virus, intrusion detection, and/or firewall software, etc.) <i>is at least one of a plurality of occurrences</i> (e.g., one of discrete events that trigger at least one of the signature/policy updates for the anti-virus, intrusion detection, and/or firewall software, etc.), <i>and the instructions include:</i></p> <p>Note: See, for example, the evidence below (emphasis added, if any):</p> <p>Note: As set forth below, a subset of intrusion-related updates (e.g., Exploit Prevention Engine information, etc.) are communicated to the Connectors.</p> <p>“Updated Exploit Prevention Engine to include changes related to the vulnerability described in CVE-2020-0796.” Cisco AMP for Endpoints Release Notes, June 25, 2020 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)</p> <p>“AMP for Endpoints Console 5.4.20200624</p> <p>Bugfixes/Updates</p> <ul style="list-style-type: none"> Fixed issue where MSSP partners were not able to see more than 25 customers on the MSSP partner page. (CSCvu61075)

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability						
	<ul style="list-style-type: none"> Updated list of processes protected by and excluded from the AMP for Endpoints Windows Exploit Prevention engine.” <p>Cisco AMP for Endpoints Release Notes, June 24, 2020 Update https://docs.amp.cisco.com/Release%20Notes.pdf</p> <p>“Deployment Options for Protection Everywhere</p> <p>Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, <u>the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:</u>”</p> <table border="1"> <thead> <tr> <th>Product Name</th><th>Details</th></tr> </thead> <tbody> <tr> <td>Cisco AMP for Endpoints</td><td><u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector</u>, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)</td></tr> </tbody> </table> <p>“Software requirements”</p> <table border="1"> <tbody> <tr> <td>Cisco AMP for Endpoints</td><td> <ul style="list-style-type: none"> Microsoft <u>Windows XP</u> with Service Pack 3 or later Microsoft <u>Windows Vista</u> with Service Pack 2 or later Microsoft <u>Windows 7</u> Microsoft <u>Windows 8 and 8.1</u> Microsoft <u>Windows 10</u> Microsoft <u>Windows Server 2003</u> </td></tr> </tbody> </table>	Product Name	Details	Cisco AMP for Endpoints	<u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector</u> , with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)	Cisco AMP for Endpoints	<ul style="list-style-type: none"> Microsoft <u>Windows XP</u> with Service Pack 3 or later Microsoft <u>Windows Vista</u> with Service Pack 2 or later Microsoft <u>Windows 7</u> Microsoft <u>Windows 8 and 8.1</u> Microsoft <u>Windows 10</u> Microsoft <u>Windows Server 2003</u>
Product Name	Details						
Cisco AMP for Endpoints	<u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector</u> , with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)						
Cisco AMP for Endpoints	<ul style="list-style-type: none"> Microsoft <u>Windows XP</u> with Service Pack 3 or later Microsoft <u>Windows Vista</u> with Service Pack 2 or later Microsoft <u>Windows 7</u> Microsoft <u>Windows 8 and 8.1</u> Microsoft <u>Windows 10</u> Microsoft <u>Windows Server 2003</u> 						

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability	
		<ul style="list-style-type: none"> • Microsoft <u>Windows Server 2008</u> • Microsoft <u>Windows Server 2012</u> • <u>Mac OS X 10.7</u> and later • <u>Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3</u> • <u>Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3</u>
	Cisco AMP for Endpoints on <u>Android</u> mobile devices	<u>Android version 2.1</u> and later
	Cisco AMP for Endpoints on <u>Apple iOS</u>	MDM supervised <u>iOS version 11</u>
<p>https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</p> <p>“Cisco’s AMP for endpoints subscription offerings begin with <u>a minimum of 50 nodes, and thus inherently the network would include a plurality of devices</u> (e.g., nodes, etc.), that include at least a first, second, and third device.”</p> <p>http://winncom.com.ua/wp-content/uploads/2018/06/Cisco-Advanced-Malware-Protection-for-Endpoints.pdf</p> <p>“<u>Correlate discrete events into coordinated attacks</u>: Cisco AMP for Networks illustrates the risk associated with an ongoing attack. It provides automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources.”</p> <p>https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)</p>		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>first instructions that, when executed by at least one first processor of the one or more processors of at least one server in communication with the at least one second storage, cause the at least one first processor to:</p> <p>generate the first vulnerability information utilizing the second vulnerability information, and</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and includes <i>first instructions</i> (e.g., server instructions, etc.) <i>that, when executed by at least one first processor of the one or more processors of at least one server</i> (e.g., one or more servers that includes, accesses, and/or serves: the Cisco AMP for Endpoints/Connectors, global intelligence database/CVE database, AMP for Endpoints Console, etc.) <i>in communication with the at least one second storage</i> (e.g., a Common Vulnerabilities and Exposures (CVE) database, etc.), <i>cause the at least one first processor to: generate the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>utilizing the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof), <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <ul style="list-style-type: none"> “AMP Cloud provides access to the global intelligence database that is constantly updated and augmented with new detections and provides a great breadth of knowledge to the AMP Connector through one-to-one hash lookups, a generic signature engine, and the machine learning engine.”

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability				
	<div data-bbox="667 305 1705 771"> <p>Shorter Time to detection Longer</p> <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid #add8e6; padding: 10px; width: 30%;"> <p style="text-align: center;">In memory</p> <div style="background-color: #90ee90; padding: 5px; margin-bottom: 5px; text-align: center;">Exploit prevention</div> <div style="background-color: #90ee90; padding: 5px; text-align: center;">System process protection</div> </div> <div style="border: 1px solid #add8e6; padding: 10px; width: 30%;"> <p style="text-align: center;">On disk</p> <div style="background-color: #00bfff; padding: 5px; margin-bottom: 5px; text-align: center;">AMP cloud</div> <div style="background-color: #00bfff; padding: 5px; margin-bottom: 5px; text-align: center;">Malicious activity protection</div> <div style="background-color: #00bfff; padding: 5px; margin-bottom: 5px; text-align: center;">TETRA</div> <div style="background-color: #00bfff; padding: 5px; text-align: center;">Custom detections</div> </div> <div style="border: 1px solid #add8e6; padding: 10px; width: 30%;"> <p style="text-align: center;">Post - infection</p> <div style="background-color: #ffa500; padding: 5px; margin-bottom: 5px; text-align: center;">Cognitive threat analytics</div> <div style="background-color: #ffa500; padding: 5px; margin-bottom: 5px; text-align: center;">Device flow correlation</div> <div style="background-color: #ffa500; padding: 5px; margin-bottom: 5px; text-align: center;">Cloud IOCs</div> <div style="background-color: #ffa500; padding: 5px; text-align: center;">Endpoint IOCs</div> </div> </div> </div> <p>https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.pdf</p> <p>“Common Vulnerabilities and Exposures</p> <p>The Common Vulnerabilities and Exposures (CVE) database records known vulnerabilities in various applications. All vulnerabilities are noted by their unique CVE ID. The CVE ID shown in the Console can be clicked to get more details on the vulnerability.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 20, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf Last Updated: December 14, 2020</p> <p>“Features and Benefits of Cisco AMP for Endpoints”</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%; text-align: left;">Feature</th><th style="width: 50%; text-align: left;">Benefits</th></tr> </thead> <tbody> <tr> <td style="height: 20px;"></td><td></td></tr> </tbody> </table>	Feature	Benefits		
Feature	Benefits				

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability	

	<u>Dashboards</u>	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, <u>as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities</u> - to provide a comprehensive contextual view so that you can make informed security decisions.

	Exploit Prevention	<u>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.</u> The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a payload, and zero-day attacks on software vulnerabilities yet to be patched.

	Vulnerabilities	Identify vulnerable software and close attack pathways. This feature <u>shows a list of hosts that contain vulnerable software, a list of the vulnerable software on each host, and the hosts most likely to be compromised.</u> Powered by our threat intelligence and security analytics, AMP identifies vulnerable software being targeted by malware, shows you the potential exploit, and provides you with a prioritized list of hosts to patch.
	https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)	
	“Introduction	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Memory attacks penetrate via endpoints and malware evades security defenses by exploiting <u>vulnerabilities in applications and operating system processes</u>. A majority of these attacks operate in the memory space of the exploited application and remain untouched by most security solutions once they gain access to the memory.”</p> <p>https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/c11-742008-00-cisco-amp-for-endpoints-wp-v2a.pdf (emphasis added)</p>
<p>communicate, from the at least one server and to the at least one of the plurality of devices over at least one network, the first vulnerability information;</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>communicate, from the at least one server</i> (e.g., the one or more servers that includes, accesses, and/or serves: the Cisco AMP for Endpoints/Connectors, global intelligence database/CVE database, AMP for Endpoints Console, etc.) <i>and to the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.) <i>over at least one network, the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth below, Cisco AMP for Endpoints includes AMP Update Server software that generates (and communicates to the Connectors/devices) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software) utilizing the second vulnerability information (e.g., ALL signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software available at the AMP Update server and/or other update servers). As set forth below, the AMP Update Server and/or other servers automatically determine which of the updates to generate and communicate.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Note: As set forth below, a subset of virus scanner updates (e.g., TETRA signatures, etc.) are communicated to the Connectors.</p> <p>“The AMP Update Server is designed to reduce the high volume of network traffic consumed by the AMP for Endpoints Windows Connector while <u>fetching TETRA definition updates from Cisco servers</u>. The utility aims to reduce the update bandwidth consumption by acting either as a caching HTTP proxy server, or by periodically fetching updates to a location that can be served by an on-premises HTTP server that you must set up and configure. You must enable your Local AMP Update Server under the TETRA section of your Windows policies. It may take an hour or longer for the AMP Update Server to download initial content from the Cisco Cloud.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 27, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>Note: As set forth below, a subset of intrusion-related updates (e.g., Exploit Prevention Engine information, etc.) are communicated to the Connectors.</p> <p>“Updated Exploit Prevention Engine to include changes related to the vulnerability described in CVE-2020-0796.”</p> <p>Cisco <i>AMP for Endpoints Release Notes</i>, June 25, 2020 Update https://docs.amp.cisco.com/Release%20Notes.pdf)</p> <p>“AMP for Endpoints Console 5.4.20200624</p> <p>Bugfixes/Updates</p> <ul style="list-style-type: none"> • Fixed issue where MSSP partners were not able to see more than 25 customers on the MSSP partner page. (CSCvu61075)

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<ul style="list-style-type: none"> • <u>Updated list of processes protected by and excluded from the AMP for Endpoints Windows Exploit Prevention engine.</u> Cisco AMP for Endpoints Release Notes, June 24, 2020 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) <p>“AMP for Endpoints Premier subscriptions include Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco AMP Efficacy Research Team to help identify threats found within the customer environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation.</p> <p>...</p> <p>Remediation includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable.” Cisco AMP for Endpoints User Guide, Chapter 28, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“Exploit Prevention (Connector version 6.0.5 and later)</p> <p>The AMP for Endpoints Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a Custom Detections - Simple list.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>To enable the exploit prevention engine, go to Modes and Engines in your policy and select Audit or Block mode. Audit mode is only available on AMP for Endpoints Windows Connector 7.3.1 and later. Earlier versions of the Connector will treat Audit mode the same as Block mode.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 7, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf Last Updated: December 14, 2020</p> <p>"AMP for Endpoints Exploit Prevention ...- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy." Page 13, https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf Last Updated: April 2020</p> <p>Note: As set forth below, a subset of firewall updates (e.g., firewall-related isolation information, etc.) are communicated to the Connectors.</p> <p>“AMP for Endpoints Console 5.4.20191001</p> <p>New</p> <ul style="list-style-type: none"> • Beta - Endpoint Isolation IP Allow lists: there is a new Endpoint Isolation IP Allow list type under Outbreak Control > Network - IP Block & Allow Lists. <ul style="list-style-type: none"> • IP lists with no ports and less than 200 IP addresses that are connected to Endpoint Isolation in policies will be migrated; IP lists that don’t meet these criteria will not be migrated and will need to be recreated as Endpoint Isolation IP Allow lists and added to the Endpoint Isolation policy. • Policies and groups using the Endpoint Isolation IP Allow lists will appear in the IP List details panel. All new IP allow lists for Endpoint Isolation must be created using this new list type.”

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p data-bbox="661 305 1493 375">Cisco <i>AMP for Endpoints Release Notes</i>, October 1, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)</p> <p data-bbox="661 418 1272 451">“AMP for Endpoints Windows Connector 7.0.5</p> <p data-bbox="661 500 722 524">New</p> <ul data-bbox="661 537 1913 764" style="list-style-type: none"> <li data-bbox="661 537 1913 607">• Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. <li data-bbox="661 613 1913 764">• System Process Protection notifications <ul data-bbox="709 654 1822 764" style="list-style-type: none"> <li data-bbox="709 654 1157 686">• are less verbose. (CSCvn41948) <li data-bbox="709 693 1822 764">• are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)” <p data-bbox="661 776 1493 846">Cisco <i>AMP for Endpoints Release Notes</i>, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)</p> <p data-bbox="661 889 1896 1190">“Blocked List Data Source enables you to select the IP blocked lists your Connectors use. If you select Custom, your Connectors will only use the IP blocked lists you have added to the policy. Choose Cisco to have your Connectors only use the Cisco Intelligence Feed to define malicious sites. The Cisco Intelligence Feed represents IP addresses determined by Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos continues to observe poor behavior related to an address it will be added back to the list. The Custom and Cisco option will allow you to use both the IP blocked lists you have added to the policy and the Cisco Intelligence Feed.”</p> <p data-bbox="661 1203 1860 1308">Cisco <i>AMP for Endpoints User Guide</i>, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p data-bbox="661 1357 1814 1388">Note: Following is evidence of other update servers (other than the AMP Update Server):</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>“North America Firewall Exceptions</p> <p>Organizations located in North America must allow connectivity from the Connector to the following servers over HTTPS (TCP 443):</p> <ul style="list-style-type: none"> • Event Server - intake.amp.cisco.com • Management Server - mgmt.amp.cisco.com • Policy Server - policy.amp.cisco.com • Error Reporting - crash.amp.cisco.com • Endpoint IOC Downloads - ioc.amp.cisco.com • Advanced Custom Signatures - custom-signatures.amp.cisco.com • Connector Upgrades - upgrades.amp.cisco.com (TCP 80 and 443) • Remote File Fetch - rff.amp.cisco.com <p>To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443:</p> <ul style="list-style-type: none"> • Cloud Host - cloud-ec.amp.cisco.com <p>For AMP for Endpoints Windows version 5.0 and higher you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:</p> <ul style="list-style-type: none"> • Cloud Host - cloud-ec-asn.amp.cisco.com • Enrollment Server - enrolment.amp.cisco.com <p>If you have TETRA enabled on any of your AMP for Endpoints Connectors you must allow access to the following server over TCP 80 and 443 for signature updates:</p> <ul style="list-style-type: none"> • Update Server - tetra-defs.amp.cisco.com <p>To use Orbital on your AMP for Endpoints Connectors, you must allow access to the following servers over TCP 443:</p> <ul style="list-style-type: none"> • Orbital Updates - orbital.amp.cisco.com • Orbital Queries - ncp.orbital.amp.cisco.com • Orbital Installer - update.orbital.amp.cisco.com

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>If you have Behavioral Protection enabled on your AMP for Endpoints Windows Connectors you need to allow access to the following server over TCP 443 for signature updates:</p> <ul style="list-style-type: none"> Behavioral Protection Signatures - apde.amp.cisco.com" <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 7, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>"Cisco-Maintained Exclusions</p> <p>Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, or other software. Click the Cisco-Maintained Exclusions button to view the list of exclusions. These cannot be deleted or modified and are presented so you can see which files and directories are being excluded for each application. <u>These exclusions may also be updated over time with improvements and new exclusions may be added for new versions of an application. When one of these exclusions is updated, any policies using the exclusion will also be updated so the new exclusions are pushed to your Connectors.</u></p> <p>Each row displays the operating system, exclusion set name, the number of exclusions, the number of groups using the exclusion set, and the number of computers using the exclusion set. You can use the search bar to find exclusion sets by name, path, extension, threat name, or SHA-256. You can also filter the list by operating system by clicking on the respective tabs."</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 3, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

	<div><div><div>“Windows Connector: Product Updates</div><div><div><div>Modes and Engines</div><div>Exclusions</div><div>Proxy</div><div>Outbreak Control</div><div>Product Updates</div><div>Advanced Settings</div></div><div><div>Product VersionNone</div><div>Update ServerNone</div><div><div>Date RangeStartEnd</div></div><div>Update Interval1 hour</div><div><input type="checkbox"/> Block Update if Reboot Required</div><div>RebootDo not reboot</div><div>Reboot Delay2 minutes</div></div></div></div><div><p>When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the Product Version dropdown menu showing which version you are going to and it will populate the Update Server so you can see where the files will be pulled from. There will also be information to show how many Connectors in groups that use the policy will require a reboot after updating.</p><p>You can then define the window in which updates are allowed to occur by choosing a Date Range. In Date Range, click Start to select a date and time for your start window and End to select a date and time for your end window. The Update Interval allows you to specify how long your Connectors will wait between checks for new product updates, including Orbital updates. This can be configured between every 30 minutes to every 24 hours to reduce network traffic.</p><p>Between the times set in the Date Range, if a Connector calls home to pick up a policy, it will pick up the product update. Because the Connector calls home at an interval dependent on the</p></div></div>
--	--

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Heartbeat Interval, you will want to plan your Update Window accordingly; that is, make sure the interval specified in the Update Window is larger than the Heartbeat Interval.</p> <p>If you are updating to version 4.3 or later of the AMP for Endpoints Windows Connector you will be presented with different reboot options. As of version 4.3 some updates may not require a reboot to take effect.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 4, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p>
<p>second instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the second instructions are executed by at least one second processor of the one or more processors of the at least one of the plurality of devices, cause the at least one second processor to:</p> <p>receive, from the at least one server and at the at least one of the plurality of devices over the at least one network, the first vulnerability information,</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and includes <i>second instructions</i> (e.g., instructions associated with a Connector, etc.) <i>that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.) <i>and that, when the second instructions</i> (e.g., instructions associated with a Connector, etc.) <i>are executed by at least one second processor of the one or more processors of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>cause the at least one second processor to: receive, from the at least one server</i> (e.g., the one or more servers that includes, accesses, and/or serves: the Cisco AMP for Endpoints/Connectors, global intelligence database/CVE database, AMP for Endpoints Console, etc.) <i>and at the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.) <i>over the at least one network, the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof),</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Note: As set forth above, Cisco AMP for Endpoints includes AMP Update Server software that generates (and communicates to the Connectors/devices) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software), which is received by the plurality of devices.</p>
store the first vulnerability information on the at least one first data storage, and	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>store the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>on the at least one first data storage</i> (e.g., memory on the at least one device, etc.), <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth above, Cisco AMP for Endpoints includes AMP Update Server software that generates (and communicates to the Connectors/devices) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software), which is received by the plurality of devices, and stored thereon for use that will be expanded upon below.</p>
receive the first vulnerability information from the at least one first data storage, the first vulnerability information being relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and excluding at least a portion	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>receive the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>from the at least one first data storage</i> (e.g., memory on the at least one device, etc.), <i>the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>being relevant to the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices;</p>	<p>application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>and excluding at least a portion of the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth above, Cisco AMP for Endpoints includes AMP Update Server software that generates (and communicates to the Connectors/devices) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software), which is received by the plurality of devices, and stored thereon for being subsequently accessed (e.g. received) for use that will be expanded upon below.</p>
<p>third instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the third instructions are executed by the at least one second processor, cause the at least one second processor to:</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and includes <i>third instructions</i> (e.g., instructions associated with anti-virus software, etc.) <i>that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.) <i>and that, when the third instructions</i> (e.g., instructions associated with anti-virus software, etc.) <i>are executed by the at least one second processor, cause the at least one second processor to: identify a first portion of the first vulnerability information</i> (e.g., a first segment of the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>that includes data inspection-related information</i> (e.g., signature/policy updates for anti-</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>identify a first portion of the first vulnerability information that includes data inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other data inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices,</p>	<p>virus software, etc.) <i>that is relevant to at least one of the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>and that excludes other data inspection-related information of the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.),</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth below, a subset of virus scanner updates (e.g., TETRA signatures, etc.) are communicated to the Connectors.</p> <p>“The AMP Update Server is designed to reduce the high volume of network traffic consumed by the AMP for Endpoints Windows Connector while <u>fetching TETRA definition updates from Cisco servers</u>. The utility aims to reduce the update bandwidth consumption by acting either as a caching HTTP proxy server, or by periodically fetching updates to a location that can be served by an on-premises HTTP server that you must set up and configure. You must enable your Local AMP Update Server under the TETRA section of your Windows policies. It may take an hour or longer for the AMP Update Server to download initial content from the Cisco Cloud.”</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	Cisco AMP for Endpoints User Guide, Chapter 27, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
identify a first occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>identify a first occurrence</i> (e.g., a first discrete event that triggers at least one of the signature/policy updates for the anti-virus software, etc.) <i>of the plurality of occurrences in connection with the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Correlate discrete events into coordinated attacks: Cisco AMP for Networks illustrates the risk associated with an ongoing attack. It provides automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources.” https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)</p>
cause a determination whether the at least one of the actual vulnerabilities relevant to the data inspection-related information is susceptible to being taken advantage of by the first occurrence identified in connection with the at least one of the plurality of devices,	Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>cause a determination whether the at least one of the actual vulnerabilities relevant to the data inspection-related information</i> (e.g., signature/policy updates for anti-virus software, etc.) <i>is susceptible to being taken advantage of by the first occurrence</i> (e.g., the first discrete event that triggers at least one of the signature/policy updates for the anti-virus software, etc.) <i>identified in connection with the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>utilizing the data inspection-related information</i> (e.g., signature/policy updates for anti-virus software, etc.);

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
utilizing the data inspection-related information;	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: The TETRA/ClamAV anti-virus software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device’s operating system) trigger a response.</p> <p>“TETRA</p> <p>TETRA is a full antivirus replacement and should never be enabled if another antivirus engine is installed. TETRA can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment.</p> <p>To enable TETRA and adjust settings go to Advanced Settings > TETRA in your policy.” Cisco AMP for Endpoints User Guide, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“Detection Engines</p> <p>Windows, Mac, and Linux Connectors have the option of enabling offline detection engines (TETRA for Windows and ClamAV for Mac and Linux) to protect the endpoint from malware without connecting to the Cisco Cloud to query each file.” Cisco AMP for Endpoints User Guide, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>fourth instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the fourth instructions are executed by the at least one second processor, cause the at least one second processor to:</p> <p>identify a second portion of the first vulnerability information that includes traffic inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other traffic inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices,</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and includes <i>fourth instructions</i> (e.g., instructions associated with intrusion-detection software, etc.) <i>that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.) <i>and that, when the fourth instructions</i> (e.g., instructions associated with intrusion-detection software, etc.) <i>are executed by the at least one second processor, cause the at least one second processor to: identify a second portion of the first vulnerability information</i> (e.g., a second segment of the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>that includes traffic inspection-related information</i> (e.g., signature/policy updates for intrusion-detection software, etc.) <i>that is relevant to at least one of the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>and that excludes other traffic inspection-related information of the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.),</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth below, a subset of intrusion-related updates (e.g., Exploit Prevention Engine information, etc.) are communicated to the Connectors.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>“Updated Exploit Prevention Engine to include changes related to the vulnerability described in CVE-2020-0796.”</p> <p>Cisco <i>AMP for Endpoints Release Notes</i>, June 25, 2020 Update https://docs.amp.cisco.com/Release%20Notes.pdf</p> <p>“AMP for Endpoints Console 5.4.20200624</p> <p>Bugfixes/Updates</p> <ul style="list-style-type: none"> • Fixed issue where MSSP partners were not able to see more than 25 customers on the MSSP partner page. (CSCvu61075) • <u>Updated list of processes protected by and excluded from the AMP for Endpoints Windows Exploit Prevention engine.</u>” <p>Cisco <i>AMP for Endpoints Release Notes</i>, June 24, 2020 Update https://docs.amp.cisco.com/Release%20Notes.pdf</p>
<p>identify a second occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>identify a second occurrence</i> (e.g., a second discrete event that triggers at least one of the signature/policy updates for the intrusion-detection software, etc.) <i>of the plurality of occurrences in connection with the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Correlate discrete events into coordinated attacks: Cisco AMP for Networks illustrates the risk associated with an ongoing attack. It provides automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources.”</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)
<p>cause a determination whether the at least one of the actual vulnerabilities relevant to the traffic inspection-related information is susceptible to being taken advantage of by the second occurrence identified in connection with the at least one of the plurality of devices, utilizing the traffic inspection-related information;</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>cause a determination whether the at least one of the actual vulnerabilities relevant to the traffic inspection-related information</i> (e.g., signature/policy updates for intrusion-detection software, etc.) <i>is susceptible to being taken advantage of by the second occurrence</i> (e.g., the second discrete event that triggers at least one of the signature/policy updates for the intrusion-detection software, etc.) <i>identified in connection with the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>utilizing the traffic inspection-related information</i> (e.g., signature/policy updates for intrusion-detection software, etc.);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: The anti-intrusion software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device's operating system) trigger a response.</p> <p>“Detect and Block Exploit Attempts</p> <p>Cisco AMP for Networks builds on the Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS). <u>When the system is deployed in line, it detects and blocks client-side exploit attempts that can lead to malicious file downloads</u>, commonly referred to as drive-by attacks. The NGIPS system can also protect against other vulnerability exploit attempts aimed at web browsers, Adobe Acrobat, Java, Flash, and other commonly targeted client applications. Acting as</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>early as possible in the attack chain, the system attempts to limit collateral damage and avoid costly cleanup efforts.”</p> <p>https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)</p> <p>“Exploit Prevention (Connector version 6.0.5 and later)</p> <p>The AMP for Endpoints Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a Custom Detections - Simple list.</p> <p>To enable the exploit prevention engine, go to Modes and Engines in your policy and select Audit or Block mode. Audit mode is only available on AMP for Endpoints Windows Connector 7.3.1 and later. Earlier versions of the Connector will treat Audit mode the same as Block mode.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 7, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“AMP for Endpoints Premier subscriptions include Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco AMP Efficacy Research Team to help identify threats found within the customer environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation.</p> <p>...</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Remediation includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable.” Cisco AMP for Endpoints User Guide, Chapter 28, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>"AMP for Endpoints Exploit Prevention ...- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy." Page 13, (https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf) Last Updated: April 2020</p>
<p>fifth instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the fifth instructions are executed by the at least one second processor, cause the at least one second processor to:</p> <p>identify a third portion of the first vulnerability information that includes firewall-related information that is relevant to at least one of the actual</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and includes <i>fifth instructions</i> (e.g., instructions associated with firewall software, etc.) <i>that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.) <i>and that, when the fifth instructions</i> (e.g., instructions associated with firewall software, etc.) <i>are executed by the at least one second processor, cause the at least one second processor to:</i></p> <p><i>identify a third portion of the first vulnerability information</i> (e.g., a third segment of the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>that includes firewall-related information</i> (e.g., signature/policy updates for firewall software, etc.) <i>that is relevant to at least one of the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), <i>and that excludes other firewall-related information of the second vulnerability information</i> (e.g., the larger “super-set” list of possible</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other firewall-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices,</p>	<p>vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.),</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth below, a subset of firewall updates (e.g., firewall-related isolation information, etc.) are communicated to the Connectors.</p> <p>“AMP for Endpoints Console 5.4.20191001</p> <p>New</p> <ul style="list-style-type: none"> • Beta - Endpoint Isolation IP Allow lists: there is a new Endpoint Isolation IP Allow list type under Outbreak Control > Network - IP Block & Allow Lists. <ul style="list-style-type: none"> • IP lists with no ports and less than 200 IP addresses that are connected to Endpoint Isolation in policies will be migrated; IP lists that don’t meet these criteria will not be migrated and will need to be recreated as Endpoint Isolation IP Allow lists and added to the Endpoint Isolation policy. • Policies and groups using the Endpoint Isolation IP Allow lists will appear in the IP List details panel. All new IP allow lists for Endpoint Isolation must be created using this new list type.” <p>Cisco AMP for Endpoints Release Notes, October 1, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>“AMP for Endpoints Windows Connector 7.0.5</p> <p>New</p> <ul style="list-style-type: none"> • Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications <ul style="list-style-type: none"> • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)” <p>Cisco AMP for Endpoints Release Notes, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)</p> <p>“Blocked List Data Source enables you to select the IP blocked lists your Connectors use. If you select Custom, your Connectors will only use the IP blocked lists you have added to the policy. Choose Cisco to have your Connectors only use the Cisco Intelligence Feed to define malicious sites. The Cisco Intelligence Feed represents IP addresses determined by Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos continues to observe poor behavior related to an address it will be added back to the list. The Custom and Cisco option will allow you to use both the IP blocked lists you have added to the policy and the Cisco Intelligence Feed.”</p> <p>Cisco AMP for Endpoints User Guide, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>Note: Following is evidence of other update servers (other than the AMP Update Server):</p> <p>“North America Firewall Exceptions</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Organizations located in North America must allow connectivity from the Connector to the following servers over HTTPS (TCP 443):</p> <ul style="list-style-type: none"> • Event Server - intake.amp.cisco.com • Management Server - mgmt.amp.cisco.com • Policy Server - policy.amp.cisco.com • Error Reporting - crash.amp.cisco.com • Endpoint IOC Downloads - ioc.amp.cisco.com • Advanced Custom Signatures - custom-signatures.amp.cisco.com • Connector Upgrades - upgrades.amp.cisco.com (TCP 80 and 443) • Remote File Fetch - rff.amp.cisco.com <p>To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443:</p> <ul style="list-style-type: none"> • Cloud Host - cloud-ec.amp.cisco.com <p>For AMP for Endpoints Windows version 5.0 and higher you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:</p> <ul style="list-style-type: none"> • Cloud Host - cloud-ec-asn.amp.cisco.com • Enrollment Server - enrolment.amp.cisco.com <p>If you have TETRA enabled on any of your AMP for Endpoints Connectors you must allow access to the following server over TCP 80 and 443 for signature updates:</p> <ul style="list-style-type: none"> • Update Server - tetra-defs.amp.cisco.com <p>To use Orbital on your AMP for Endpoints Connectors, you must allow access to the following servers over TCP 443:</p> <ul style="list-style-type: none"> • Orbital Updates - orbital.amp.cisco.com • Orbital Queries - ncp.orbital.amp.cisco.com • Orbital Installer - update.orbital.amp.cisco.com <p>If you have Behavioral Protection enabled on your AMP for Endpoints Windows Connectors you need to allow access to the following server over TCP 443 for signature updates:</p> <ul style="list-style-type: none"> • Behavioral Protection Signatures - apde.amp.cisco.com"

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“Cisco-Maintained Exclusions</p> <p>Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, or other software. Click the Cisco-Maintained Exclusions button to view the list of exclusions. These cannot be deleted or modified and are presented so you can see which files and directories are being excluded for each application. <u>These exclusions may also be updated over time with improvements and new exclusions may be added for new versions of an application. When one of these exclusions is updated, any policies using the exclusion will also be updated so the new exclusions are pushed to your Connectors.</u></p> <p>Each row displays the operating system, exclusion set name, the number of exclusions, the number of groups using the exclusion set, and the number of computers using the exclusion set. You can use the search bar to find exclusion sets by name, path, extension, threat name, or SHA-256. You can also filter the list by operating system by clicking on the respective tabs.”</p> <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 3, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p>
identify a third occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and	Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>identify a third occurrence</i> (e.g., a third discrete event that triggers at least one of the signature/policy updates for the firewall software, etc.) <i>of the plurality of occurrences in connection with the at least one of the plurality of devices</i> (e.g., one of the 50+ nodes licensed to use the software, etc.), and

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Correlate discrete events into coordinated attacks: Cisco AMP for Networks illustrates the risk associated with an ongoing attack. It provides automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources.” https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)</p>
<p>cause a determination whether the at least one of the actual vulnerabilities relevant to the firewall-related information is susceptible to being taken advantage of by the third occurrence identified in connection with the at least one of the plurality of devices, utilizing the firewall-related information; and</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>cause a determination whether the at least one of the actual vulnerabilities relevant to the firewall-related information (e.g., signature/policy updates for firewall software, etc.) is susceptible to being taken advantage of by the third occurrence (e.g., the third discrete event that triggers at least one of the signature/policy updates for the firewall software, etc.) identified in connection with the at least one of the plurality of devices (e.g., one of the 50+ nodes licensed to use the software, etc.), utilizing the firewall-related information (e.g., signature/policy updates for firewall software, etc.); and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: The firewall software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device’s operating system) trigger a response.</p> <p>“Firewall Connectivity</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>To allow the AMP for Endpoints Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are three sets of servers depending on where you are located: one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world.</p> <p>IMPORTANT! If your firewall requires IP address exceptions, see this Cisco TechNote.” Cisco AMP for Endpoints User Guide, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“AMP for Endpoints Windows Connector 7.0.5</p> <p>New</p> <ul style="list-style-type: none"> • Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications <ul style="list-style-type: none"> • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)” <p>Cisco AMP for Endpoints Release Notes, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)</p>
sixth instructions that, when executed by at least one third processor of an administrator computer, cause the at least one third processor to:	Cisco Advanced Malware Protection (AMP) infringes claim 1 and includes <i>sixth instructions</i> (e.g., Endpoints Console-related instructions embedded in a web page accessible via a browser for accessing the AMP for Endpoints Console, etc.) <i>that, when executed by at least one third processor of an administrator computer</i> (e.g., a machine with a browser for accessing the AMP for Endpoints Console, etc.), <i>cause the at least one third processor to: in response to administrator action</i> (e.g., user input, etc.), <i>cause setting, before the first occurrence</i> (e.g., the

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>in response to administrator action, cause setting, before the first occurrence, of a first policy for the third instructions that is applied to a group including each of the plurality of devices that has the at least one operating system installed thereon,</p>	<p>first discrete event that triggers at least one of the signature/policy updates for the anti-virus software, etc.), <i>of a first policy</i> (e.g., a policy for anti-virus software, etc.) <i>for the third instructions</i> (e.g., instructions associated with anti-virus software, etc.) <i>that is applied to a group including each of the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.) <i>that has the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>installed thereon</i>,</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“System Requirements</p> <p>To access the AMP for Endpoints Console, you will need one of the following Web browsers:</p> <ul style="list-style-type: none"> • Internet Explorer 11 or higher • Microsoft Edge 38.14393 or higher • Mozilla Firefox 14 or higher • Apple Safari 6 or higher • Google Chrome 20 or higher” <p>Cisco <i>AMP for Endpoints User Guide</i>, Chapter 1, https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p> <p>“Policy Summary</p> <p>Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>in response to administrator action, cause setting, before the second occurrence, of a second policy for the fourth instructions that is applied the group including each of the plurality of devices that has the at least one operating system installed thereon,</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to, <i>in response to administrator action</i> (e.g., user input, etc.), <i>cause setting, before the second occurrence</i> (e.g., the second discrete event that triggers at least one of the signature/policy updates for the intrusion-detection software, etc.), <i>of a second policy</i> (e.g., a policy for intrusion-detection software, etc.) <i>for the fourth instructions</i> (e.g., instructions associated with intrusion-detection software, etc.) <i>that is applied the group including each of the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.) <i>that has the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>installed thereon</i>,</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Policy Summary</p> <p>Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<div><h3>Policies</h3><div><div>View All Changes</div><div>Search</div><div>All ProductsWindowsAndroidMacLinuxiOS</div><div>New Policy...</div></div><div><div>Audit</div><div>This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ...</div><div><div>Modes and Engines</div><div>Exclusions</div><div>Proxy</div><div>Groups</div></div><div><div>Files</div><div>Audit</div><div>Workstation Exclusions</div><div>Not Configured</div><div>Audit</div><div>8</div></div><div><div>Network</div><div>Audit</div><div></div><div></div><div>Beta Features Root Group</div><div>0</div></div><div><div>TETRA</div><div>On</div><div></div><div></div><div></div><div></div></div><div><div>Exploit Prevention</div><div>Off</div><div></div><div></div><div></div><div></div></div></div><div><div>Outbreak Control</div><div>Custom Detections - Simple</div><div>Custom Detections - Advanced</div><div>Application Control</div><div>Network</div></div><div><div>File Blacklist</div><div>Not Configured</div><div>Execution Blacklist</div><div>blacklist</div><div>Not Configured</div></div><div><div>File Whitelist</div><div></div><div>whitelist</div><div></div><div></div></div></div> <div><div>View Changes</div><div>Modified 2017-12-01 20:59:11 UTC</div><div>Serial Number 2</div><div>Download XML</div><div>Duplicate</div><div>Edit</div><div>Delete</div></div> <div><p>View Changes will take you to a filtered view of the Audit Log showing all the changes for that specific policy. You can also use View All Changes at the top of the page to show changes to all policies.</p><p>Click Edit to modify an existing policy or click Duplicate if you want to create a new policy with the same settings.”</p><p>Cisco AMP for Endpoints User Guide, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p></div>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>in response to administrator action, cause setting, before the third occurrence, of a third policy for the fifth instructions that is applied to the group including each of the plurality of devices that has the at least one operating system installed thereon, and</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to, <i>in response to administrator action</i> (e.g., user input, etc.), <i>cause setting, before the third occurrence</i> (e.g., the third discrete event that triggers at least one of the signature/policy updates for the firewall software, etc.), <i>of a third policy</i> (e.g., a policy for firewall software, etc.) <i>for the fifth instructions</i> (e.g., instructions associated with firewall software, etc.) <i>that is applied to the group including each of the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.) <i>that has the at least one operating system</i> (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>installed thereon, and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Policy Summary</p> <p>Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
<p>cause the utilization of the different occurrence mitigation actions of the diverse occurrence mitigation types, including the firewall-based occurrence mitigation type and the other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing the advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.</p>	<p>Cisco Advanced Malware Protection (AMP) infringes claim 1 and is configured to <i>cause the utilization of the different occurrence mitigation actions of the diverse occurrence mitigation types</i> (e.g., firewall software-, intrusion detection software-, anti-virus software-related actions, etc.), <i>including the firewall-based occurrence mitigation type</i> (e.g., applying signature/policy updates for firewall software, etc.) <i>and the other occurrence mitigation type</i> (e.g., applying signature/policy updates for intrusion-detection software, etc.), <i>across the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.) <i>for occurrence mitigation by preventing the advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types</i> (e.g., firewall software-, intrusion detection software-, anti-virus software-related actions, etc.) <i>across the plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Policy Summary</p> <p>Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 2 Elements	Applicability
	<p>The Outbreak Control menu contains items related to controlling outbreaks in your network.</p> <ul style="list-style-type: none"> • Custom Detections <ul style="list-style-type: none"> ○ Simple to convict files that are not yet classified. ○ Advanced to create signatures that will detect parts of the Portable Executable (PE) file. ○ Android to warn of new threats or unwanted apps. • Application Control <ul style="list-style-type: none"> ○ Blocked Lists to stop executables from running. ○ Allowed Lists to create lists of applications that will not be wrongly detected. • Network <ul style="list-style-type: none"> ○ IP Blocked & Allowed Lists allow you to explicitly detect or allow connections to specified IP addresses. • Endpoint IOC <ul style="list-style-type: none"> ○ Initiate Scan to schedule and start IOC scans on your AMP for Endpoints Connectors (Administrator only). ○ Installed Endpoint IOCs to upload new endpoint IOCs and view installed endpoint IOCs (Administrator only). ○ Scan Summary to view the results of endpoint IOC scans. • Automated Actions <ul style="list-style-type: none"> ○ Automated Actions lets you set actions that automatically trigger when a specified event occurs on a computer.” <p>Cisco AMP for Endpoints User Guide, Chapter 1, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020</p>

Caveat: The notes and/or cited excerpts utilized herein are set forth for illustrative purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Cisco Advanced Malware Protection (AMP) for Endpoints

excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same in connection with any subsequent correlations.